CHAPTER 3

PART ONE

PHYSICAL SECURITY MEASURES

0300. SECURITY MEASURES

a. Physical security measures are necessary to establish or maintain an adequate command physical security posture. Where appropriate and feasible, physical security measures are to be coordinated and integrated on a regional basis.

b. Physical security measures are a combination of active or passive systems, devices, and security personnel used to protect a security interest from possible threats. These measures include:

(1) Security forces and owner or user personnel.

(2) Military working dogs.

(3) Physical barriers, facility hardening and active delay or denial systems.

(4) Secure locking systems, containers, and vaults.

(5) Intrusion detection systems.

(6) Assessment or surveillance systems (i.e., closed-circuit television or thermal imagers).

(7) Protective lighting.

(8) Badging systems, access control devices, material or asset tagging systems, and contraband detection equipment.

0301. ANTITERRORISM AND FORCE PROTECTION MEASURES. Antiterrorism and force protection standards and measures are addressed in references (g) through (j).

0302. SECURITY OF FUNDS. Unless more specific measures are prescribed by other authorities, funds including cash and readily negotiable instruments will be protected in a manner that is clearly appropriate for the amount of money involved. Commanding officers shall not send armed money escorts off base without approval from the local authorities and/or the regional commander.

0303. LOSS REPORTING. Requirements and guidelines for reporting loss of arms, ammunition and explosives are outlined in reference (e).

0304. KEY SECURITY AND LOCK CONTROL. Each Navy activity must establish a key and lock control program for all keys, locks, padlocks and locking devices used to meet security and loss prevention objectives of this manual. It is not intended to include keys, locks and padlocks used for convenience, privacy, administrative, or personal use.

a. Reference (e) governs controls and security of keys and locks used to provide security of arms, ammunition, and explosives.

b. Keys and locks cannot be adequately controlled without inventories. The frequency of inventories shall be appropriate for the local circumstances, especially circumstances that exacerbate problems of maintaining control.

c. No key and lock control program can assure that any given key has not been compromised over a period of time. Accordingly, where padlocks and removable lock cores are used, there must be a program to rotate these locks and cores. The intent is that anyone possessing a key without authorization eventually discovers that the location of the lock which the key fits is no longer known. If the rotation is done in conjunction with lock maintenance, the incremental impact on resources including manpower should be minimal. This approach is more cost effective than replacing all existing keys and replacing or rekeying all existing locks.

d. All locks and padlocks used to meet standards in this manual shall be adequate for the intended security of the protected asset. To this end, the activity security officer should be involved in the lock procurement process so that only locks that are adequate for their intended application are procured.

e. Lockouts. If a lock does not work properly, do not assume the reasons are innocent ones. Although the failure of a locking device could be the result of a product failure, it could alternately be a result of attempted or actual illegal penetration. Therefore, all lockouts involving locks used to meet security objectives of this manual will be promptly examined by competent personnel to determine the cause of the lockout and the security officer notified of the determination.

0305. SECURITY CHECKS. Each Navy activity must establish a system for the checking by occupants/users of restricted areas, facilities, containers, and barrier or building entry and departure points to detect any deficiencies or violations of security standards.

CHAPTER 3

PART TWO

SECURITY OF AIRCRAFT, SHIPS IN PORT, AND OTHER WEAPON SYSTEMS AND PLATFORMS ASHORE

0306. GENERAL. This part establishes policy and responsibility for security of aircraft, ships in port, and other weapon systems and platforms ashore.

0307. POLICY

a. Installation commanding officers are responsible for the security of assets whether assigned or transient while these assets are resident on their installations. Commanding officers shall develop security plans to meet this responsibility.

b. The priority for security placed on similar assets within the Echelon 2 command may vary due to differences in the following:

(1) Mission;

(2) Location and vulnerability;

(3) Operational readiness;

(4) Value, classification, and replacement costs.

c. Before operations commence, the command (or Service) owning the assets should request any special security support from the host installation, if necessary, as far in advance as possible. Economic and logistical considerations dictate that every reasonable effort be made by the host installation to provide the necessary security without resort to external support from the command owning the asset (aircraft, ship, etc.). The owning command should provide material and personnel for extraordinary security measures (extraordinary security measures are those that require heavy expenditures of funds, equipment, or manpower; or unique or unusual technology) to the host installation.

0308. AIRCRAFT SECURITY PLANNING. In general planning for aircraft security, an installation commander should consider the degree to which the installation provides a secure environment. Installation commanders should consider at least the following factors:

a. Whether the installation is open or closed to the public.

b. Whether the flightline or aircraft parking area is adequately fenced, lighted, and posted with signs.

c. Whether a controlled access policy or limited entry restriction is in effect at the flightline or aircraft parking area.

d. Whether, and to what degree, the flightline or aircraft parking area has security or law enforcement patrol coverage or surveillance provided by personnel working within or around the area.

e. Intrusion Detection Systems (IDS) should be used to augment other physical security procedures, devices, and equipment.

0309. TRANSIENT OR DEPLOYED AIRCRAFT

a. The installation commander will always provide a secure area for transient aircraft on the installation.

b. For administrative aircraft, this requirement may be met by parking aircraft in an area where normal personnel activity provides a reasonable degree of deterrence.

c. More critical aircraft require additional security measures as listed below. The host installation should make every reasonable effort to provide the same degree of security that the owning Service would provide under the same (transient or deployed) circumstances.

(1) Park the aircraft in a permanent restricted area with an IDS when possible.

(2) If it is not possible to park the aircraft in an established restricted area with IDS, park it in a hangar or encircle it with an elevated barrier, such as rope and stanchions. When a hangar is used, the walls constitute the restricted area boundary.

(3) Provide area lighting of sufficient intensity to allow the security force to detect and track intruders.

(4) Display restricted area signs so that personnel approaching the aircraft can see the signs.

(5) Provide circulation control. Entry must be limited to only those persons who have a need to enter.

(6) Require the senior security supervisor to give the aircraft commander a local threat assessment for the duration of ground time.

0310. OTHER SITUATIONS

a. Various aircraft assigned to the Services provide tactical support, logistical support, reconnaissance, and

refueling capability for worldwide American interests. Many of these aircraft, because of their large size or mission tasking, are an attractive target. This is particularly true at installations where their presence is unusual, they are on display, or are located at civilian or foreign airfields. Refer to the security requirements matrix (table 3-1) to determine the minimum security to be provided for nonalert aircraft. These requirements apply to aircraft on display or located at civilian or foreign airfields. Special or increased requirements for specific operational configuration must be identified in advance (when possible) to host security forces.

b. Security forces in support of aircraft must be notified before a visit to the aircraft is allowed to take place. Any change in security priorities based on operational status must be identified to the host installation.

c. The aircraft commander determines if security is adequate.

0311. EMERGENCY SITUATIONS

a. Initial security for aircraft that crash or are forced to land outside a military installation is the responsibility of the nearest military installation. The owning Service will respond and assume on-site security as soon as possible.

b. In the above emergency situations, security must:

(1) Ensure the safety of civilian sightseers.

(2) Prevent tampering with or pilfering from the aircraft.

(3) Preserve the accident scene for later investigation.

(4) Protect classified cargo and aircraft components.

0312. STANDOFF

a. The standoff zone, also referred to as the setback area, is the second tier of defense and includes that space between the outer perimeter of the site and the exterior of what you are protecting. Standoff zones provide time delays and more importantly, abatement of blast effects.

b. To mitigate the effectiveness of a vehicle bomb attack, commanders shall be continually vigilant against allowing vehicle parking near high density buildings and on piers. Every attempt should be made to establish minimum standoff distances, which vary depending on the type of construction, level of protection desired and proximity of perimeter barriers. It is important to understand that explosive effects decay with

increased distance. The following are recommended minimum distances:

(1) Structural:

- 80 feet during THREATCON ALPHA*
- 100 feet during THREATCON BRAVO
- 400 feet during THREATCONs CHARLIE and DELTA

All new construction, facility modifications and MILCON projects shall comply with paragraphs 0120, 0121 and 0122 of this manual as well as the Deputy Under Secretary of Defense for Installations, Interim DoD Antiterrorism/Force Protection Construction Standards of 16 Dec 99.

* Unless otherwise hardened in compliance with DoD standards cited above.

(2) Pierside:

- 50 feet during THREATCON NORMAL
- 100 feet during THREATCONs ALPHA and BRAVO
- 400 feet during THREATCONs CHARLIE and DELTA

Every effort should be made to achieve 100 foot CONUS and 400 foot OCONUS standoff as written in OPNAVINST 3300.55 'NAVY COMBATING TERRORISM PROGRAM STANDARDS'. Distances are only applicable when an asset is present at pier.

(3) Waterside:

- 100 feet during THREATCON NORMAL
- 200 feet during THREATCONs ALPHA and BRAVO
- 400 feet during THREATCONs CHARLIE and DELTA

The above waterside standoff distances represent the outboard dimension of the innermost zone. Achievable standoff may vary based on existing structures, proximity of navigable waterways and/or as allowed by host nation agreements.

0313. HARBOR SURVEILLANCE AND WATERSIDE/WATERWAY SECURITY. Commanding officers will ensure waterways adjacent to afloat assets are under appropriate surveillance, and where possible and as the threat dictates, or as otherwise directed, adequately patrolled.

Aircraft Type	Security Priority	Entry Control Responsibility	SRT[1] Team	CBS[2]	Motorized Patrol
Tactical Aircraft (AV-8, F-14, F/A-18)	C	Aircrew	Yes	—	Yes
Airlift Aircraft (C-3, C-9, C-130, C-141)	C	Aircrew	Yes	—	Yes
Strategic Bomber Aircraft (B-1, FB-111)	C	Aircrew	Yes	—	Yes
Air Refueling Aircraft (KA-6, KC-10, KC-135)	C	Aircrew	Yes	—	Yes
Special Mission Aircraft (E-2, EA-6, EP-3, ES-3)	B	Security	Yes	Yes	—
Reconnaissance Aircraft (S-3, P-3)	B	Security	Yes	Yes	—
Advanced Technology Aircraft	B	Pilot carries detailed information for divert contigencies	—	—	—
Other DoD Aircraft	C	Aircrew	Yes	Yes	Yes

[1] Security Response Team (SRT). A team consisting of two security force members available to respond within 5 minutes. All priority aircraft require SRT support. SRTs may be area patrols not specifically dedicated to the visiting aircraft.

[2] Close Boundary Sentry (CBS). A security force member posted inside or outside the boundary to keep the boundary of the restricted area under surveillance.

CHAPTER 3

PART THREE

PROTECTION OF BULK PETROLEUM PRODUCTS

0314. GENERAL. This part prescribes general policies for security of Government-owned, Government-operated (GOGO) and Government-owned, Contractor-operated (GOCO) fuel support points, pipeline pumping stations, and piers.

0315. POLICY

a. Commanders of GOGO and GOCO fuel support points, pipeline pumping stations, and piers shall designate and post these installations as Restricted Areas. (This restricted area requirement does not apply to locations for issue (and incidental storage) of ground fuels for use in motor vehicles, material handling equipment, and stationary power and heating equipment. Commanding officers will determine the means to protect against loss or theft of fuel at these locations.)

b. Access to these facilities shall be controlled and only authorized personnel shall be permitted to enter. Commanders shall determine the means required to enforce access control (i.e., security forces, barriers, lighting, and security badges) based on the considerations in Chapter 2 of this Instruction.

0316. SECURITY PLAN AND LIAISON. Commanders shall take the following actions to protect their fuel facilities:

a. Establish liaison and coordinate contingency plans and inspection requirements with the nearest U.S. military installation to provide manpower and equipment resources to the facility in the event of emergencies and increased threat conditions.

b. Establish liaison with supporting law enforcement agencies and host nation officials; and support agreements, if appropriate.

0317. PHYSICAL SECURITY INSPECTIONS

a. Navy installations responsible for the security oversight of fuel facilities will conduct a physical security inspection of that facility at least once every 2 years.

b. Inspections should be formal, recorded assessments of crime prevention measures and other physical security measures, used to protect the facilities from loss, theft, destruction, sabotage, or compromise.

CHAPTER 3

PART FOUR

SECURITY OF COMMUNICATIONS SYSTEMS

0318. GENERAL

a. This part describes concepts for physical security of communications facilities located on and off Navy installations, to include mobile systems. Specific security support for facilities that require special security measures shall be coordinated between or among the concerned activities and installations.

b. Because of the difference in location, physical layout and equipment, security considerations must be thoroughly assessed for each communications system. The physical security program shall be tailored to that particular facility or system.

0319. POLICY

a. The protection provided to communication facilities and systems shall be sufficient to ensure continuity of operations of critical users and the facilities they support. These include nuclear weapon delivery units and storage facilities and primary command and control elements. The determinations on strategic importance, both to the United States and its allies, shall be based upon whether or not each mobile system or facility processes, transmits, or receives, telecommunications traffic considered crucial by the National Command Authorities, the Chairman, Joint Chiefs of Staff, or the Commanders in Chief of the Unified and Specified Commands. Commander, Naval Computer and Telecommunications Command shall be consulted on this issue.

b. Communications systems play a major role in support of each Navy activity's mission, providing operational communications in both peacetime and wartime. These are attractive targets due to limited staffing, isolated location and mission. Therefore, security for these systems must be an important part of each command's physical security program.

c. Parent Echelon 2 commands must review the host installation's implementation of physical security measures during inspections, oversight, and staff visits.

d. Access shall be controlled at all communications facilities; only authorized personnel shall be allowed to enter. Facilities should be designated and posted as Restricted Areas.

e. Depending on regional conditions, commanders should consider locating enough weapons and ammunition at communications facilities to arm designated onsite personnel. If arms are

stored at the facilities, appropriate security measures and procedures shall be employed following reference (e). Weapons will not be located at unmanned facilities.

f. Existing essential structures should be hardened against attacks. This includes large antenna support legs, antenna horns, operations building and cable trays. Future construction programs for critical communications facilities should include appropriate hardening of essential structures.

0320. RESPONSIBILITIES. Fleet Commanders in Chief and other Echelon 2 commands will:

a. Identify critical communications facilities and mobile systems within their commands.

b. Ensure that a security plan is developed for each communications facility and mobile system within their command. The plan shall include emergency security actions and procedures for emergency destruction of sensitive equipment and classified information. The plan may be an annex to an existing host installation security plan; only the applicable parts of the total plan shall be distributed to personnel at the facility or mobile system.

c. Arrange for security of off-installation facilities and mobile systems with the closest U.S. military installation. This includes contingency plans for manpower and equipment resources during emergencies. These arrangements can be made by establishing a formal agreement such as an interservice support agreement. Whether the facilities are located on or off the installation, or mobile, installation commanders are responsible for security of communications facilities for which they provide host support.

d. Because operations, maintenance, and communications personnel at the facility or mobile system are the most important factor in security, ensure implementation of a training program to ensure that assigned personnel understand their day-to-day security responsibilities, are familiar with the vulnerabilities of the facility, and are prepared to implement emergency security actions. The training program shall include the following:

(1) Security procedures and personal protection skills for assigned personnel.

(2) The use of weapons and communications equipment for protecting the facility or mobile system.

(3) Awareness of local terrorist threats and other activity in the area.

0321. MOBILE COMMUNICATIONS SYSTEMS. Per chapter 2 of this instruction, a security operational concept or standards shall be developed for mobile systems to describe the minimum level of security for the system in the expected operational environment.

CHAPTER 3

PART FIVE

SECURITY OF MATERIEL

0322. GENERAL. This part provides security policy and procedures for safeguarding controlled inventory items, including drugs, drug abuse items, (as identified under Code of Federal Regulations (CFR), 21 CFR 1301.71 through 1301.76 and P.L. 91-513), and precious metals. The following definitions describe sensitive items:

(1) Selected Sensitive Inventory Items. Those items security coded "Q" or "R" in the Defense Integrated Data System that are controlled substances, drug abuse items, or precious metals.

(2) Code "Q" Items. Drug or other controlled substances designated as Schedule III, IV, or V items, per 21 CFR 1308.

(3) Code "R" Items. Precious metals and drugs or other controlled substances designated as Schedule I or II items per 21 CFR 1308.

(4) Precious Metals. Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granule, liquid, sponge, or wire form.

0323. POLICY

a. The security of controlled inventory items is of special concern to the DoD. Consequently, these items shall have characteristics so that they can be identified, accounted for, secured or segregated to ensure their protection and integrity.

b. Special attention shall be paid to the safeguarding of inventory items by judiciously implementing and monitoring physical security measures. This shall include analysis of loss rates through inventories, reports of surveys, and criminal incident reports, to establish whether repetitive losses indicate criminal or negligent activity.

0324. RESPONSIBILITIES

a. Commanding officers shall:

(1) Establish physical security measures to protect inventory items, and to reduce the incentive and opportunity for theft.

(2) Monitor the effective implementation of security requirements through scheduled inspections of and staff or oversight visits to affected activities.

(3) Ensure that adequate safety and health considerations are incorporated into the construction of a security area for controlled inventory items.

(4) Ensure that storage facilities and procedures for operation adequately safeguard controlled inventory items.

0325. Controlled Substances Inventory. Accountability and inventory of controlled substances shall be as prescribed in reference (o).

0326. SECURITY REQUIREMENTS FOR "R" CODED ITEMS AT BASE AND INSTALLATION SUPPLY LEVEL OR HIGHER

a. Storage in vaults or strongrooms (as defined in reference (a)) or 750 pound or heavier General Services Administration (GSA)-approved security containers. Smaller GSA-approved security containers are authorized, but must be securely anchored to the floor or wall. All security containers will be secured with built-in Group One combination locks. Or they may be stored using any means which provide a degree of security equivalent to any of the preceding.

b. Unless not feasible, storage areas or containers will be protected with an installed intrusion detection system.

0327. SECURITY REQUIREMENTS FOR "Q" CODED ITEMS AT BASE AND INSTALLATION SUPPLY LEVEL OR HIGHER

a. The preferred storage for sensitive inventory items coded "Q" is in vaults or strongrooms (as defined in reference (a)).

b. Small quantities may be stored in security containers or other means approved for items coded "R."

0328. SECURITY REQUIREMENTS FOR "R" AND "Q" CODED ITEMS BELOW BASE AND INSTALLATION LEVEL (i.e., Small Unit/Individual Supplies)

a. Storage as described in paragraphs 0326 and 0327.

b. As an alternative, small stocks may be stored in a 750-pound or heavier GSA-approved security container. Smaller GSA-approved security containers are authorized, but must be securely anchored to the floor or wall. Also, any means which provides a degree of security equivalent to any of the preceding may be used. Security containers should also be located within a continuously manned space or be checked by a

security force member at least twice per 8-hour shift, barring any reason for the contrary.

0329. LOSS PREVENTION MEASURES. A loss prevention program is essential at every Navy activity. Losses of property may prevent timely accomplishment of mission requirements.

a. The mission is affected not only by direct loss of the property, but it is also affected by lost opportunities of procuring other goods and services to improve mission accomplishment because available funds must be diverted to loss replacement. A manager whose property must be continually bought over and over again to replace losses is robbing other managers of the opportunity of putting the same money to better use.

b. As a minimum, loss prevention measures will consist of the following:

(1) To identify trends and patterns of losses, there must be a continuing process of loss analysis. It should consider the types of material lost; geographic location; times and dates; proximity of specific personnel; proximity of doorways, passageways, loading docks and ramps, gates, parking facilities, piers and other activities adjacent to loss or gain locations; material movement paths; etc.

(2) It is intended that the results of analysis of loss and gain trends and patterns will be used to appropriately allocate resources available for crime prevention.

(3) Actions to prevent or reduce opportunities for losses of government property at supply centers, shipyards, shipping and receiving points, ordnance stock points, and other Navy activities, should be stressed.

(4) Warehouses, storage buildings, office buildings, and other structures which contain high value, sensitive, or pilferable property, supplies, or office equipment are to be afforded security protection commensurate with the value and sensitivity of the contents.

(5) Shore activities that are tenants may need to include loss prevention support in host-tenant agreements or inter-service support agreements. Where feasible and appropriate, such support should be coordinated and integrated among Navy activities on a regional basis.

(6) Employees must be made continually aware of the need for loss prevention and local procedures for preventing property losses as well as their responsibility for the care and protection of government property.